UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

EFREN RAMOS,

Plaintiff,

v.

THE GAP, INC.,

Defendant.

Case No. 23-cv-04715-HSG

ORDER GRANTING SECOND MOTION TO DISMISS

Re: Dkt. No. 49

Pending before the Court is Defendant The Gap Inc.'s second motion to dismiss. Dkt. No. 49. The Court finds this matter appropriate for disposition without oral argument and the matter is deemed submitted. *See* Civil L.R. 7-1(b). For the reasons detailed below, the Court **GRANTS** the motion.

I. BACKGROUND

Plaintiff Efren Ramos initially filed this putative class action in September 2023. *See* Dkt. No. 1. Defendant moved to dismiss the complaint in its entirety, and the Court granted the motion. *See* Dkt. No. 40. In October 2024, Plaintiff filed an amended complaint. *See* Dkt. No. 41 ("FAC"). As before, Plaintiff alleges that Defendant invades customers' privacy through the use of third-party tracking software. *See generally id.* Defendant is a clothing retailer that, as relevant to this lawsuit, sends its customers periodic marketing emails that contain hyperlinks to products on Defendant's website.[1] *See id.* at ¶ 2.

According to the FAC, Defendant contracts with a third party, Bluecore, Inc., to embed "invisible pixels" and URLs in Defendant's marketing emails. *See id.* at ¶¶ 3, 5, 18–19. Plaintiff

[1] The email domain is bananarepublicfactory@email.bananarepublicfactory.com and the website is at https://bananarepublicfactory.gapfactory.com.

alleges that these pixels and URLs "are connected to" the hyperlinked images and text in the marketing emails such that when a customer clicks on an image or text in an email, "the URL is transmitted to Bluecore." *See id.* at ¶ 3. Moreover, Plaintiff alleges that each URL is unique such that Bluecore knows "exactly when a customer opens one of its Emails along with the exact images and words that a consumer clicked on before being routed to Defendant's website . . . ." *Id.* at ¶¶ 4, 19, 27, 45. Plaintiff alleges that in this way Bluecore knows, for example, that Plaintiff clicked on a specific shirt in one of Defendant's marketing emails. *See id.* at ¶ 12. Plaintiff also alleges that each link is "numbered and mapped" in such a way that Bluecore knows "its location within the email." *See id.* at ¶¶ 33–34, & n.19. Bluecore also captures other information like the customer's email address, email open rates, and content click rates before redirecting the recipient to Defendant's website. *See id.* at ¶¶ 19, 21, 29–35. With all this information, Plaintiff alleges that "Bluecore is able to create . . . a replica of how Defendant's recipients are seeing and interacting with the Emails' Content in real time." *Id.* at ¶ 40.

Plaintiff alleges that Bluecore also uses JavaScript and other "persistent cookies" to continue to monitor customers as they navigate on Defendant's website "throughout their purchase journey." *See id.* at ¶¶ 22, 36–38. According to the FAC, Bluecore aggregates the data from a customer's interaction with Defendant's emails and website to create a "highly detailed personal profile" of each customer. *See id.* at ¶¶ 5, 38.

Based on these allegations, Plaintiff brings causes of action against Defendant for (1) violations of the California Invasion of Privacy Act ("CIPA"), Cal Penal Code §§ 631(a) and 635; (2) statutory larceny, Cal. Penal Code §§ 486 and 496; and (3) violations of the California Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code §§ 17200, *et seq*. Defendant again has moved to dismiss the complaint. *See* Dkt. No. 49.

II. LEGAL STANDARD

Federal Rule of Civil Procedure 8(a) requires that a complaint contain "a short and plain statement of the claim showing that the pleader is entitled to relief." Fed. R. Civ. P. 8(a)(2). A defendant may move to dismiss a complaint for failing to state a claim upon which relief can be granted under Rule 12(b)(6). "Dismissal under Rule 12(b)(6) is appropriate only where the complaint lacks a cognizable legal theory or sufficient facts to support a cognizable legal theory." *Mendiondo v. Centinela Hosp. Med. Ctr.*, 521 F.3d 1097, 1104 (9th Cir. 2008). To survive a Rule 12(b)(6) motion, a plaintiff need only plead "enough facts to state a claim to relief that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). A claim is facially plausible when a plaintiff pleads "factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009).

Rule 9(b) imposes a heightened pleading standard where fraud is an essential element of a claim. *See* Fed. R. Civ. P. 9(b) ("In alleging fraud or mistake, a party must state with particularity the circumstances constituting fraud or mistake."); *see also Vess v. Ciba–Geigy Corp. USA*, 317 F.3d 1097, 1107 (9th Cir. 2003). A plaintiff must identify "the who, what, when, where, and how" of the alleged conduct, so as to provide defendants with sufficient information to defend against the charge. *Cooper v. Pickett*, 137 F.3d 616, 627 (9th Cir. 1997). However, "[m]alice, intent, knowledge, and other conditions of a person's mind may be alleged generally." Fed. R. Civ. P. Rule 9(b).

In reviewing the plausibility of a complaint, courts "accept factual allegations in the complaint as true and construe the pleadings in the light most favorable to the nonmoving party." *Manzarek v. St. Paul Fire & Marine Ins. Co.*, 519 F.3d 1025, 1031 (9th Cir. 2008). Nevertheless, courts do not "accept as true allegations that are merely conclusory, unwarranted deductions of fact, or unreasonable inferences." *In re Gilead Scis. Secs. Litig.*, 536 F.3d 1049, 1055 (9th Cir. 2008) (quoting *Sprewell v. Golden State Warriors*, 266 F.3d 979, 988 (9th Cir. 2001)).

III. DISCUSSION

A. CIPA

Plaintiff alleges that Defendant's conduct constitutes an illegal wiretap under CIPA § 631(a). *See* FAC at ¶¶ 55–65. Section 631(a) contains four distinct clauses, imposing liability on "any person" who:

(i) "by means of any machine, instrument, or contrivance, or in any other manner, intentionally taps . . . any telegraph or telephone wire, line, cable, or instrument";

> (ii) "willfully reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit";
>
> (iii) "uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained"; and
>
> (iv) "aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above."

Cal. Penal Code § 631(a); *see also Tavernetti v. Superior Ct.*, 22 Cal. 3d 187, 192 (Cal. 1978) (en banc) (clarifying that § 631(a) imposes liability for "distinct and mutually independent patterns of conduct: intentional wiretapping, willfully attempting to learn the contents or meaning of a communication in transit over a wire, and attempting to use or communicate information obtained as a result of engaging in either of the previous two activities."). Plaintiff continues to allege that Defendant is liable under all four clauses. *See* FAC at ¶¶ 55–65; Dkt. No. 51 at 4–13.

i. Direct Liability

A party to the communication cannot be held liable under § 631(a). *See In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 607 (9th Cir. 2020) (citing *Warden v. Kahn*, 99 Cal. App. 3d 805, 811 (Cal. Ct. App. 1979)). Although Plaintiff appears to ground the FAC on a theory that Defendant "aided and abetted" Bluecore's wiretapping, *see* FAC at ¶ 1, the opposition to the motion to dismiss outlines two theories of direct liability against Defendant. *See* Dkt. No. 51 at 3–4. The Court finds both theories confusing and unsupported by the FAC.

First, Plaintiff suggests that Defendant tapped "the private communications between Plaintiff and the Class Members (on the one hand) and their respective email providers (on the other)" by tracking when a Class Member opened one of Defendant's marketing emails. Dkt. No. 51 at 3. This theory is not alleged in the FAC, and Plaintiff's attempt to rewrite this allegation in the opposition is improper. *See, e.g.*, FAC at ¶ 3 ("Bluecore wiretaps and intercepts Plaintiff's and Class Members' email communications with *Defendant*.") (emphasis added). But even if Plaintiff had adequately alleged this theory, the Court does not find it plausible. As the Court previously explained, email open rates are not content. *See* Dkt. No. 40 at 8–9. Plaintiff's theory, if accepted, would transform the routine routing of emails into standalone communications between email providers and their users. Plaintiff has offered no support for stretching CIPA so far.

Second, Plaintiff suggests that Defendant tapped third-party emails whenever a Class Member forwarded one of Defendant's marketing emails to another person. *See* Dkt. No. 51 at 4. In the order granting the first motion to dismiss, the Court suggested that Plaintiff may be able to allege a plausible claim giving rise to direct liability under § 631(a) if Plaintiff could show that Bluecore's software allowed Defendant to view "information about *third-party* emails in Plaintiff's inbox, and not just those from Defendant." Dkt. No. 40 at 4 (emphasis in original). In his opposition, Plaintiff contends that this occurs when "a Class Member forwards one of the Emails containing the Bluecore spyware to a friend." Dkt. No. 51 at 4. But the FAC does not contain any allegations that such forwarding ever occurred.[2] And even if it did, Plaintiff has not explained how this would transform a marketing email from Defendant into a third-party email. The Court further rejects Plaintiff's suggestion that he is somehow entitled to discovery to augment his complaint and theories of liability. *See id.* Plaintiff cannot cycle through theories of liability with the hope of stumbling upon one that can withstand a motion to dismiss.

The Court therefore **GRANTS** the motion to dismiss to the extent Plaintiff attempts to hold Defendant directly liable under § 631(a).

ii. Communications over the Internet: Clause One

The first clause of § 631(a) provides for the punishment by fine or imprisonment of "any person who by means of any machine, instrument, or contrivance, or in any other manner, intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively, or otherwise, with any *telegraph or telephone* wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system." Cal. Penal Code § 631(a) (emphasis added). The Court previously found that the first

[2] Plaintiff points to a single sentence in the FAC that Defendant can "track its known, *and unknown*, userbase." *See* Dkt. No. 51 at 4 (citing FAC at ¶ 62) (emphasis in original). This cannot fairly be read to allege that anyone forwarded one of Defendant's marketing emails, let alone that in doing so, Defendant intercepted a third-party email. As the Court previously explained, "[n]either Defendant nor the Court should have to guess about such a fundamental piece of Plaintiff's case." *See* Dkt. No. 40 at 8.

clause does not apply to internet communications. *See* Dkt. No. 40 at 5–7. Although Plaintiff insists that "a closer reading of the statute" should lead to a different result, *see* Dkt. No. 51 at 4–5, the Court already considered Plaintiff's arguments and simply disagrees. The Court **GRANTS** the motion to dismiss on this basis.

iii. Protected Content: Clauses Two through Four

Clauses two and three of § 631(a) prohibit the unauthorized access to and use of the "contents" of any communications, and clause four prohibits aiding and abetting such conduct. Cal. Penal Code § 631(a). The definition of "contents" under CIPA is the same as under the Electronic Communications Privacy Act ("ECPA"). *See, e.g.*, *In re Google RTB Consumer Priv. Litig.*, 606 F. Supp. 3d 935, 949 (N.D. Cal. 2022). The Ninth Circuit has held that under the ECPA "'contents' refers to the intended message conveyed by the communication, and does not include record information regarding the characteristics of the message that is generated in the course of the communication." *In re Zynga Priv. Litig.*, 750 F.3d 1098, 1106 (9th Cir. 2014). In other words, courts must consider whether the intercepted information is "information *about* a user's communication, or "the communication itself." *Id.* at 1107 (emphasis added). Only the latter is protected under CIPA.

Defendant argues that the FAC—like the original complaint—does not allege the wiretapping of protected "contents" under CIPA. *See* Dkt. No. 49 at 9–10. Plaintiff's theories are difficult to pin down, and Plaintiff appears to go out of his way to avoid identifying with any specificity the purported communications at issue here. But as best as the Court can discern, Plaintiff contends that (1) a user's "click" on a URL contained within Defendant's marketing emails is itself content; and (2) the URLs reveal the content of Defendant's marketing emails such that Bluecore can somehow "read" the actual marketing emails. The Court is not persuaded by either theory.

First, Plaintiff contends that a user's "click" on the embedded URLs within the marketing emails is a communication or "response" to Defendant that Bluecore intercepted. *See* Dkt. No. 51 at 8, 12–13. Plaintiff contends that clicking on the URL is the equivalent of a user saying, "I am interested in learning more about this shirt, please send me more information." Dkt. No. 51 at 8;

see also FAC at ¶ 59 ("Bluecore was able to identify the contents of Plaintiff and the Class Members' response to the Emails—*i.e.*, their intent to view, purchase or learn more about the exact items showcased in the Emails."). Plaintiff urges that clicking on an embedded URL in Defendant's emails is the "modern alternative to manually replying to Defendant requesting additional information about the featured inventory or asking for a contract to purchase." *See id.* at 8–9.

The Court simply is not convinced by Plaintiff's characterization of the click of the embedded URL as a communication between Plaintiff and Defendant. As alleged, the marketing emails contain hyperlinked text and images that, when clicked, allow users to navigate to a specific webpage on Defendant's website (*e.g.*, to a specific article of clothing). *See* FAC at ¶¶ 2, 30, 38. As such, and as the Court previously explained, the URLs appear to serve a tracking or routing function. *See* Dkt. No. 40 at 10. Under Plaintiff's new theory, however, any "click" on a URL would be a communication that the user is interested in the information linked in the URL. But the Ninth Circuit has not drawn such sweeping conclusions.

To the contrary, in *Zynga*, the Ninth Circuit disagreed with the plaintiffs that information obtained by clicking on a web address fell within the definition of protected "content." *See Zynga*, 750 F.3d at 1106–09. Zynga was a game developer that offered free social gaming applications on Facebook's platform. *See id.* at 1101–02. To play, a user would click on a link to the game application from a Facebook webpage. *See id.* According to the plaintiffs, Zynga programmed its gaming applications to collect information about users from this click, including the user's Facebook ID and the address of the Facebook webpage that the user was viewing when he or she clicked on the game link. *See id.* Zynga then sent this information to third-party advertisers. *See id.* at 1102. But the Ninth Circuit held that this information was not protected content. *See id.* at 1106–09. The court reasoned that the Facebook ID only "function[ed] as a 'name' or a 'subscriber number or identity.'" *Id.* at 1107. And likewise, the webpage "identifie[d] the location of a webpage a user [was] viewing on the internet, and therefore function[ed] like an 'address.'" *Id.*

The Ninth Circuit contrasted this with examples in which a plaintiff sends "an email message saying 'here's my Facebook ID number,' or 'you have to check out this website'" or fills out an online form with personal information. *See id.* (citing *In re Pharmatrak, Inc.*, 329 F.3d 9, 18–19 (1st Cir. 2003)). The plaintiffs in these examples are plainly communicating. *Id.* Similarly, the court distinguished cases in which a URL captures the specific search terms that a user entered into a search engine. *Id.* at 1107–09 (citing *In re Application of U.S. for an Ord. Authorizing use of A Pen Reg. & Trap On (XXX) Internet Serv. Acct./User Name, (xxxxxxxx@xxx.com)*, 396 F. Supp. 2d 45, 49 (D. Mass. 2005)). The court explained that "a user's request to a search engine for specific information could constitute a communication such that divulging a URL containing that search term to a third party could amount to disclosure of the contents of a communication." *Id.* at 1108–09.

Plaintiff attempts to distinguish *Zynga* in a single sentence. He asserts that here, "clicking on any of the URLs contained in the Email discloses *why* a customer arrived at the exact subpage on Defendant's Website (due to their response to Defendant's private email communication) rather than *how* they arrived to the Website (without revealing any other substantive information)." *See* Dkt. No. 51 at 11 (emphasis in original). But Plaintiff's attempt to distinguish between "why" a user arrived on a webpage and "how" he arrived there seems purely a matter of semantics. One could just as easily argue that in *Zynga*, clicking on the application revealed "why" a user arrived at the specific online game: the user was interested in that game and clicked on a link from a specific webpage. At bottom, Plaintiff offers nothing more than his unsupported assertion that clicking on the URLs in the marketing emails here—which direct the user to Defendant's website—constitutes a communication from Plaintiff to Defendant.[3] This is not enough. *See In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 604–05 (9th Cir. 2020) (distinguishing between URLs collected in *Zynga*, "which revealed only that a Facebook user had clicked on a

[3] This argument appears particularly strained given that Plaintiff alleges that he and other putative class members were unaware of Bluecore's tracking software. *See* FAC at ¶¶ 3–5. Plaintiff characterizes the use of this software as a "secret," which is "virtually untraceable" and "functions effectively to permit Defendant and Bluecore to stand over the shoulder of Plaintiff and Class Members to view what emails they choose to open, read, engage with, reply to, as well as how they engage with those e mails." *See id.* at ¶¶ 7, 35. But if Plaintiff was unaware that Defendant (through Bluecore) was tracking his engagement with its marketing emails, it is not clear how Plaintiff could intend to communicate anything to Defendant by clicking on a URL link in those same emails. *Cf. Zynga*, 750 F.3d at 1106 (interpreting "the word 'contents' to mean a person's intended message to another").

link to a gaming website," with URLs that could include "search terms inputted into a third-party search engine"); *St. Aubin v. Carbon Health Techs., Inc.*, No. 24-CV-00667-JST, 2024 WL 4369675, at *4–5 (N.D. Cal. Oct. 1, 2024) (same) (collecting cases).

Plaintiff's second argument seems even more contrived. Plaintiff argues that the URLs in the marketing emails allowed Bluecore to "read" the substance of Defendant's marketing emails because "the URLs are merely proxies for the specific image or words clicked on by the recipient." *See* FAC at ¶ 27. Plaintiff repeats this allegation in several different ways:

- "The URLs and pixels are connected to the images that the customer or prospective customer sees in the Email such that when a customer clicks on the image within the Email to navigate to Defendant's website, the URL is transmitted to Bluecore, which corresponds to the image within the Email." *See id.* at ¶ 3.
- "[B]y embedding a unique URL behind the hyperlinked text and images, when Plaintiff clicked on a hyperlink, Bluecore could identify the exact image or text that Plaintiff clicked on (*e.g.*, a specific shirt) . . . ." *Id.* at ¶ 12.
- "The invisible URL links allow Bluecore to identify the particular contents of the email the customer or prospective customer clicked on, as well as which specific customer clicked on it." *Id.* at ¶ 19.
- "Bluecore embeds hidden URL links within the clickable images and words of an email (*i.e.*, the email's content because the hidden URL corresponds to the specific hyperlinked image or words contained within the body of the email)." *Id.* at ¶ 38.
- "The embedded URLs convey the intended message within the Email communications because they permitted Bluecore to identify the exact image or text (*e.g.*, a specific shirt) that Plaintiff and the Class Members received and clicked on before their computers were redirected to the web page they originally sought to navigate to (*i.e.*, the exact subpage of the precise items being clicked on within the emails)." *Id.* at ¶ 59.

Despite the repetition, this appears to be just another way of saying that the embedded

URLs allow Bluecore to determine which link(s) Plaintiff and putative class members clicked on. *See, e.g.*, *id.* at ¶ 19 ("When the recipient of an email clicks on a trackable URL link, the customers are directed to Bluecore's servers, permitting Bluecore to capture a large amount of data, such as the recipient's email address as well as email open rates, and content click rates."); *id.* at ¶ 38 ("When a user clicks on the content of the email to be directed to a particular webpage within a website (*e.g.*, a specific shirt showcased in the email), Bluecore immediately intercepts the contents of the communication *and* gathers valuable data by receiving the full detailed URLs (including the exact subpage of the precise items being purchased or viewed) . . . ."). As already explained, such clicks are not protected content.

This is further reinforced by Plaintiff's description of the information actually conveyed by the URLs at issue here. Plaintiff broadly alleges that a URL can be broken down into the scheme, domain name, path, and query parameters. *See id.* at ¶¶ 28, 30. However, none of these elements allegedly "read" the contents of the email such that they intercept the actual "substance, purport, or meaning" of Defendant's emails. *Zynga*, 750 F.3d at 1104; *see also* Dkt. No. 40 at 10–11.

- Scheme: A scheme "[s]pecifies the method used to access the resource (e.g., http, https)." *Id.* at ¶ 28.
- Domain: A domain is "[t]he address of the server where the resource is hosted." *See id.* at ¶ 28. In this context, the domain is the Banana Republic Factory website, https://bananarepublicfactory.gapfactory.com/. *See id.* at ¶¶ 13, 30.
- Path: The path is "[t]he specific location of the resource on the server." *See id.* at ¶ 28. This is the specific webpage on the Banana Republic Factory website containing the specific article of clothing. *See id.* at ¶¶ 30, 38.
- Parameters: Parameters include "[a]dditional contextual data passed to the server." *See id.* at ¶ 28. Here, Plaintiff suggests that this may include information such as the "source of the [website] traffic," such as the marketing email; the "campaign" for which the email was sent (*e.g.*, a "fall sale" clothing campaign); "which part of the email was clicked"; and "[a] unique identifier for the recipient" of the email.

See id. at ¶¶ 29, 30.

Plaintiff's bare contrary assertion that Bluecore's software allows it to "read" the marketing emails is not enough to state a plausible claim.

To the extent the FAC suggests that Bluecore actually knows what Defendant's marketing emails say, it is not because of the information allegedly contained in and shared through the URLs. Rather, Plaintiff alleges that Bluecore helps *create* the marketing emails. *See id.* at ¶ 25 ("Emails embedded with Bluecore's spyware are created either by Defendant's marketing team or Bluecore, who create the design and layout of the Email (including text, images, buttons, and other visual assets)."). The emails are uploaded to Bluecore's "Visual Template Editor," which embeds the URLs into the emails, and then the emails are ultimately sent through Bluecore's own platform. *See id.* at ¶¶ 19–20, 25–26, 29, 31, 40. Plaintiff also acknowledges that Bluecore "retains a visual copy of the Emails" on its own servers. *See id.* at ¶ 27. In other words, Bluecore creates both the emails and the URLs. Given this framework, even as alleged Bluecore has no need to recreate the marketing emails by piecing together information from the link(s) that Plaintiff may click on.[4]

And the cases that Plaintiff cites do not support his theory. For example, in *Campbell v. Facebook, Inc.*, the plaintiff alleged that Facebook "scanned" the content of private messages that users sent to each other on Facebook's social media website. 315 F.R.D. 250, 255 (N.D. Cal. 2016). According to the complaint, Facebook was scanning the messages for links to other webpages. *Id.* Facebook would treat the link as a "like" of the webpage, and would further share this data with third parties to compile user profiles to deliver "targeted advertising." *See id.* at

[4] There appear to be several other flaws with this theory. Even if Bluecore did somehow reconstruct the marketing emails from a user's URL click, it is not clear how Bluecore could still be said to have read the contents of the email "while the same is in transit" as required under CIPA. *See* Cal. Penal Code § 631(a). Plaintiff also contends that despite Bluecore's heavy involvement in the creation and distribution of the marketing emails, the emails and the URLs within them nevertheless "belong to Defendant rather than Bluecore." *See* Dkt. No. 51 at 6. However, Plaintiff does not point to any allegations in the FAC that actually support this assertion. Bluecore is also alleged to have a licensing agreement with Defendant, *see* FAC at ¶ 10, which further muddles whether Bluecore is even a third party to these marketing emails at all.

255–57. In *Campbell*, the plaintiff directly alleged that Facebook was scanning or reading the actual messages that users were sending each other. And the URLs were not "embedded links" like those at issue here, but rather were a substantive part of the users' private messages.

Plaintiff also cites *In re Meta Pixel Healthcare Litigation*, in which Meta allegedly obtained health information about the plaintiffs from their health providers' online patient portals. *See* 647 F. Supp. 3d 778, 784, 795–96 (N.D. Cal. 2022). According to the plaintiffs, their health providers used the "Meta Pixel" on their websites, which would send information back to Meta. *See id.* at 784–85. The Pixel enabled Meta to obtain information about patient status by capturing when a user logged into the patient portal and the URL from the patient portal. *See id.* at 785–86, 791–92. The Pixel also sent information to Meta about what the patient browsed on the patient portal, including doctors, medical conditions, and appointments. *See id.* The plaintiffs further alleged that Meta monetized this information by using it for targeted advertising on and off Facebook. *See id.* at 785–86. The plaintiffs' expert, for example, explained that within two hours of searching for information on ulcerative colitis on the hospital's website, he was shown advertisements related to ulcerative colitis on Facebook. *See id.* at 786.

The court in *In re Metal Pixel* concluded that the log-in buttons and descriptive URLs that Meta obtained constituted content for purposes of CIPA because they contained the "query string," which included any searches the user may have done on the healthcare provider's website. *See id.* at 795–96, & n.10. As such, the court reasoned that they constituted the communication between the user and the patient portal. *Id.* Here, however, Plaintiff has not alleged that such communicative information was transmitted through the URLs to Bluecore. As discussed above, the URLs were either created by or with Bluecore, and linked (*i.e.*, functioned like an address) to products on Defendant's website.[5]

[5] Plaintiff does not meaningfully argue that Bluecore collected protected content on Defendant's website. *See* Dkt. No. 51 at 5–13. In response to Plaintiff's prior arguments, the Court previously explained that Plaintiff "[did] not allege that he ever entered any information into a popup on Defendant's website." *See* Dkt. No. 40 at 11. And he similarly failed to provide any "detail about his use of Defendant's website." *See id.* The FAC still only contains generic information that "Bluecore continued to intercept Mr. Ramos's communications with Defendant's website, such as the web pages (corresponding to the specific shirt in the Email) viewed by Plaintiff." *See* FAC at ¶ 12; *see also id.* at ¶¶ 42, 58–59.

While a robust policy debate could be had about whether it is a net positive or negative that so much online activity can be tracked, the Court's task is solely to determine whether doing so is a violation of CIPA. Plaintiff has not met his burden of alleging that it does, even when liberally construing the FAC as the Court must at this stage. The Court therefore **GRANTS** the motion to dismiss on this basis.

iv. CIPA § 635

Because the Court agrees with Defendant that Plaintiff has failed to plead the interception of protected content under § 631(a), the Court similarly **GRANTS** the motion to dismiss Plaintiff's derivative claim under § 635.

B. Statutory Larceny

Plaintiff also alleges that Defendant's conduct here constitutes statutory larceny. *See* FAC at ¶¶ 72–84. Specifically, Plaintiff alleges that Defendant "stole, took, and/or fraudulently appropriated Plaintiff and the Class members' personal information without their consent" and for Defendant's own financial benefit. *See* FAC at ¶¶ 81–82. California Penal Code § 484 prohibits theft of personal property through "false or fraudulent representations or pretense." Cal. Penal Code § 484(a). California Penal Code § 496(a), in turn, prohibits the receipt of "any property that has been stolen or that has been obtained in any manner constituting theft . . . ." Cal. Penal Code § 496(a). It is not clear whether Plaintiff believes, as Defendant does, that his statutory larceny claim is dependent on his § 631(a) claim. In any event, the parties also dispute whether the information allegedly obtained by Bluecore constitutes property for purposes of §§ 484 and 496.

According to Defendant, "property" must be "capable of *exclusive* possession or control . . . ." *See* Dkt. No. 49 at 12 (quoting *Lau v. Gen Digital Inc.*, No. 22-CV-08981-RFL, 2024 WL 1880161, at *4 (N.D. Cal. Apr. 3, 2024)) (emphasis added). Defendant argues that Plaintiff's online data, including his browsing history, "is shared with a variety of service providers that facilitate access to the website at issue," and thus is not within anyone's exclusive possession or control. *Id.* Plaintiff does not appear to dispute that exclusive possession or control is necessary to allege a statutory larceny claim. *See* Dkt. No. 51 at 14–15; *see also G.S. Rasmussen & Assocs., Inc. v. Kalitta Flying Serv., Inc.*, 958 F.2d 896, 903 (9th Cir. 1992) (noting that under California law a property right "must be capable of exclusive possession or control"). Instead, he suggests that he has pled such exclusivity.

Plaintiff states that Defendant stole information "directly from his private email account." *See id.* at 15. He urges that he "had a legitimate exclusivity claim in his email data . . . ." *Id.* He suggests that Bluecore's software "caused Plaintiff's email provider to communicate with Bluecore's domain without his consent—this is akin to a person hacking into a private email account and sending unauthorized emails." *See id.* The Court finds Plaintiff's argument difficult to follow and unsupported by any authority. Like Plaintiff's CIPA claim, Plaintiff provides few citations to the FAC to support his assertions. Moreover, Plaintiff offers no explanation why the "email data" that Defendant allegedly took was property that could be exclusively possessed or controlled, beyond his *ipse dixit* conclusion. The Court **GRANTS** the motion to dismiss Plaintiff's statutory larceny claim.

C. Unfair Competition Law (UCL)

Lastly, Plaintiff alleges that Defendant violated the UCL. *See* FAC at ¶¶ 85–97. In response, Defendant raises both procedural and substantive arguments. *See* Dkt. No. 49 at 12–15. However, because the UCL claim is dependent on Plaintiff's CIPA and statutory larceny claims, Plaintiff's UCL claim similarly fails. Plaintiff suggests that even if his CIPA and statutory larceny claims fail, some aspect of his UCL claim—particularly under the "unfair" prong—could survive because "Defendant's business practices could nonetheless have violated other subsections of CIPA as well as other claims that Plaintiff could have plausibly raised in the FAC . . . ." *See* Dkt. No. 51 at 17. But the question is not whether Plaintiff *could* plead a UCL claim based on some other violations or unfair conduct, but whether he in fact did so. Plaintiff offers no explanation as to how the FAC, as drafted, adequately alleges a UCL claim if his CIPA and statutory larceny claims fail. Nor does he explain how he could amend the complaint to support such a claim if given leave to do so. In short, Plaintiff has not adequately alleged that Defendant's conduct violates the UCL, and the Court **GRANTS** the motion to dismiss on this basis.

IV. CONCLUSION

The Court **GRANTS** the motion to dismiss. Dkt. No. 49. Particularly given the expansive implications of Plaintiff's theory, the Court expects more from counsel than the scattershot and vague assertions presented here. Both the FAC and Plaintiff's opposition to the motion to dismiss read as if counsel is continuously shapeshifting in search of a legal theory that can be stretched to cover the facts of this case. But Plaintiff has had ample opportunity to amend the complaint and has failed to cure the deficiencies that the Court previously identified. The Court therefore **DISMISSES** the case against Defendant without leave to amend. *See Ramirez v. Galaza*, 334 F.3d 850, 860 (9th Cir. 2003) ("Leave to amend should be granted unless the pleading could not possibly be cured by the allegation of other facts, and should be granted more liberally to pro se plaintiffs.") (quotations omitted); *Zucco Partners, LLC v. Digimarc Corp.*, 552 F.3d 981, 1007 (9th Cir. 2009) ("[W]here the Plaintiff has previously been granted leave to amend and has subsequently failed to add the requisite particularity to its claims, [t]he district court's discretion to deny leave to amend is particularly broad." (quotation omitted)). The Clerk is directed to enter judgment in favor of Defendant The Gap, Inc. and against Plaintiff and to close the case.

IT IS SO ORDERED.

Dated: 7/29/2025

Haywood S. Gill Jr.

HAYWOOD S. GILLIAM, JR.
United States District Judge